Foundation of Cryptography (0368-4162-01), Lecture 3

Hardcore Predicates for Any One-way Function

Iftach Haitner, Tel Aviv University

November 15, 2011

Definition 1 (hardcore predicates)

An efficiently computable function $b : \{0,1\}^n \mapsto \{0,1\}$ is an hardcore predicate of $f : \{0,1\}^n \mapsto \{0,1\}^n$, if

$$\Pr[P(f(U_n)) = b(U_n)] \leq \frac{1}{2} + \operatorname{neg}(n),$$

for any PPT P.

Definition 1 (hardcore predicates)

An efficiently computable function $b : \{0,1\}^n \mapsto \{0,1\}$ is an hardcore predicate of $f : \{0,1\}^n \mapsto \{0,1\}^n$, if

$$\Pr[P(f(U_n)) = b(U_n)] \leq \frac{1}{2} + \operatorname{neg}(n),$$

for any PPT P.

Theorem 2

Let $f \colon \{0,1\}^n \mapsto \{0,1\}^n$ be a OWF, and define $g \colon \{0,1\}^n \times \{0,1\}^n \mapsto \{0,1\}^n \times \{0,1\}^n$ as $g(x,r) = f(x), r$. Then $b(x,r) = \langle x, r \rangle_2$, is an hardcore predicate of g.

Note that if f is one-to-one, then so is g.

Section 1

The Information Theoretic Case

Definition 3 (min-entropy)

The min entropy of a random variable X, is defined

$$\mathrm{H}_{\infty}(X) := \min_{y \in \mathrm{Supp}(X)} \log \frac{1}{\Pr_X[y]}.$$

Definition 3 (min-entropy)

The min entropy of a random variable X, is defined

$$\mathrm{H}_\infty(X) := \min_{y \in \mathrm{Supp}(X)} \log \frac{1}{\Pr_X[y]}.$$

Examples

Pairwise independent hashing

Definition 4 (pairwise independent hash functions)

A function family $\mathcal{H}$ from $\{0,1\}^n$ to $\{0,1\}^m$ is pairwise independent, if for every $x \neq x' \in \{0,1\}^n$ and $y, y' \in \{0,1\}^m$, it holds that $\Pr_{h \leftarrow \mathcal{H}}[h(x) = y \wedge h(x') = y')] = 2^{-2m}$.

Pairwise independent hashing

Definition 4 (pairwise independent hash functions)

A function family $\mathcal{H}$ from $\{0,1\}^n$ to $\{0,1\}^m$ is pairwise independent, if for every $x \neq x' \in \{0,1\}^n$ and $y, y' \in \{0,1\}^m$, it holds that $\Pr_{h \leftarrow \mathcal{H}}[h(x) = y \wedge h(x') = y')] = 2^{-2m}$.

Lemma 5 (leftover hash lemma)

Let X be a random variable over $\{0,1\}^n$ with $\mathrm{H}_\infty(X) \geq k$ and let $\mathcal{H}$ be a family of pairwise independent hash functions from $\{0,1\}^n$ to $\{0,1\}^m$, then

$$\mathrm{SD}((h, h(x))_{h \leftarrow \mathcal{H}, x \leftarrow X}, (h, y)_{h \leftarrow \mathcal{H}, y \leftarrow \{0,1\}^m}) \leq 2^{(m-k-2))/2}.$$

Pairwise independent hashing

Definition 4 (pairwise independent hash functions)

A function family $\mathcal{H}$ from $\{0,1\}^n$ to $\{0,1\}^m$ is pairwise independent, if for every $x \neq x' \in \{0,1\}^n$ and $y, y' \in \{0,1\}^m$, it holds that $\Pr_{h \leftarrow \mathcal{H}}[h(x) = y \wedge h(x') = y')] = 2^{-2m}$.

Lemma 5 (leftover hash lemma)

Let X be a random variable over $\{0,1\}^n$ with $\mathrm{H}_\infty(X) \geq k$ and let $\mathcal{H}$ be a family of pairwise independent hash functions from $\{0,1\}^n$ to $\{0,1\}^m$, then

$$\mathrm{SD}((h, h(x))_{h \leftarrow \mathcal{H}, x \leftarrow X}, (h, y)_{h \leftarrow \mathcal{H}, y \leftarrow \{0,1\}^m}) \leq 2^{(m-k-2))/2}.$$

* We typically simply write $\mathrm{SD}((H, H(X)), (H, U_m))$, where H is uniformly distributed over $\mathcal{H}$.

efficient function families

Definition 6 (efficient function family)

An ensemble of function families $\mathcal{F} = \{\mathcal{F}_n\}_{n\in\mathbb{N}}$ is efficient, if the following hold:

Samplable. $\mathcal{F}$ is samplable in polynomial-time: there exists a PPT that given 1^n, outputs (the description of) a uniform element in $\mathcal{F}_n$.

Efficient. There exists a polynomial-time algorithm that given $x \in \{0,1\}^n$ and (a description of) $f \in \mathcal{F}_n$, outputs $f(x)$.

hardcore predicate for regular OWF

Lemma 7

Let $f:\{0,1\}^n \mapsto \{0,1\}^n$ be a $d(n) \in 2^{\omega(\log n)}$ regular function and let $\mathcal{H} = \{\mathcal{H}_n\}$ be an efficient family of Boolean pairwise independent hash functions over $\{0,1\}^n$. Define $g\colon \{0,1\}^n \times \mathcal{H}_n \mapsto \{0,1\}^n \times \mathcal{H}_n$ as

$$g(x,h) = (f(x), h),$$

then $b(x,h) = h(x)$ is an hardcore predicate of g.

hardcore predicate for regular OWF

Lemma 7

Let $f : \{0,1\}^n \mapsto \{0,1\}^n$ be a $d(n) \in 2^{\omega(\log n)}$ regular function and let $\mathcal{H} = \{\mathcal{H}_n\}$ be an efficient family of Boolean pairwise independent hash functions over $\{0,1\}^n$. Define $g\colon \{0,1\}^n \times \mathcal{H}_n \mapsto \{0,1\}^n \times \mathcal{H}_n$ as

$$g(x,h) = (f(x),h),$$

then $b(x,h) = h(x)$ is an hardcore predicate of g.

How does it relate to the computational case?

hardcore predicate for regular OWF

Lemma 7

Let $f : \{0,1\}^n \mapsto \{0,1\}^n$ be a $d(n) \in 2^{\omega(\log n)}$ regular function and let $\mathcal{H} = \{\mathcal{H}_n\}$ be an efficient family of Boolean pairwise independent hash functions over $\{0,1\}^n$. Define $g \colon \{0,1\}^n \times \mathcal{H}_n \mapsto \{0,1\}^n \times \mathcal{H}_n$ as

$$g(x,h) = (f(x),h),$$

then $b(x,h) = h(x)$ is an hardcore predicate of g.

How does it relate to the computational case?

Proof: We prove the claim by showing that

Claim 8

$\mathrm{SD}\left((f(U_n), H, H(U_n)), (f(U_n), H, U_1)\right) = \mathrm{neg}(n)$, where the rv $H = H(n)$ is uniformly distributed over $\mathcal{H}_n$.

hardcore predicate for regular OWF

Lemma 7

Let $f : \{0,1\}^n \mapsto \{0,1\}^n$ be a $d(n) \in 2^{\omega(\log n)}$ regular function and let $\mathcal{H} = \{\mathcal{H}_n\}$ be an efficient family of Boolean pairwise independent hash functions over $\{0,1\}^n$. Define $g \colon \{0,1\}^n \times \mathcal{H}_n \mapsto \{0,1\}^n \times \mathcal{H}_n$ as

$$g(x,h) = (f(x),h),$$

then $b(x,h) = h(x)$ is an hardcore predicate of g.

How does it relate to the computational case?

Proof: We prove the claim by showing that

Claim 8

$\mathrm{SD}\left((f(U_n), H, H(U_n)), (f(U_n), H, U_1)\right) = \mathrm{neg}(n)$, where the rv $H = H(n)$ is uniformly distributed over $\mathcal{H}_n$.

Does this conclude the proof?

Proving Claim 8

Proof: For $y \in \{f(x)\colon x \in \{0,1\}^n\}$, let the rv X_y be uniformly distributed over $f^{-1}(y) := \{x \in \{0,1\}^n\colon f(x) = y\}$.

Proving Claim 8

Proof: For $y \in \{f(x) \colon x \in \{0,1\}^n\}$, let the rv X_y be uniformly distributed over $f^{-1}(y) := \{x \in \{0,1\}^n \colon f(x) = y\}$.

$$\begin{aligned}
&\mathrm{SD}((f(U_n), H, H(U_n)), (f(U_n), H, U_1)) \\
&= \sum_{y \in f(\{0,1\}^n)} \Pr[f(U_n) = y] \cdot \mathrm{SD}\big((f(U_n), H, H(U_n) \mid f(U_n) = y) \\
&\qquad\qquad , (f(U_n), H, U_1 \mid f(U_n) = y)\big)
\end{aligned}$$

Proving Claim 8

Proof: For $y \in \{f(x) \colon x \in \{0,1\}^n\}$, let the rv X_y be uniformly distributed over $f^{-1}(y) := \{x \in \{0,1\}^n \colon f(x) = y\}$.

$$
\begin{aligned}
&\mathrm{SD}((f(U_n), H, H(U_n)), (f(U_n), H, U_1)) \\
&\quad = \sum_{y \in f(\{0,1\}^n)} \Pr[f(U_n) = y] \cdot \mathrm{SD}\big((f(U_n), H, H(U_n) \mid f(U_n) = y) \\
&\qquad\qquad\qquad\qquad\qquad , (f(U_n), H, U_1 \mid f(U_n) = y)\big) \\
&\quad = \sum_{y \in f(\{0,1\}^n)} \Pr[f(U_n) = y] \cdot \mathrm{SD}\left((y, H, H(X_y)), (y, H, U_1)\right)
\end{aligned}
$$

Proving Claim 8

Proof: For $y \in \{f(x) \colon x \in \{0,1\}^n\}$, let the rv X_y be uniformly distributed over $f^{-1}(y) := \{x \in \{0,1\}^n \colon f(x) = y\}$.

$$
\begin{aligned}
&\mathrm{SD}((f(U_n), H, H(U_n)), (f(U_n), H, U_1)) \\
&\quad= \sum_{y \in f(\{0,1\}^n)} \Pr[f(U_n) = y] \cdot \mathrm{SD}\big((f(U_n), H, H(U_n) \mid f(U_n) = y) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad , (f(U_n), H, U_1 \mid f(U_n) = y)\big) \\
&\quad= \sum_{y \in f(\{0,1\}^n)} \Pr[f(U_n) = y] \cdot \mathrm{SD}\left((y, H, H(X_y)), (y, H, U_1)\right) \\
&\quad\leq \max_{y \in f(\{0,1\}^n)} \mathrm{SD}((y, H, H(X_y)), (y, H, U_1))
\end{aligned}
$$

Proving Claim 8

Proof: For $y \in \{f(x) \colon x \in \{0,1\}^n\}$, let the rv X_y be uniformly distributed over $f^{-1}(y) := \{x \in \{0,1\}^n \colon f(x) = y\}$.

$$
\begin{aligned}
&\mathrm{SD}((f(U_n), H, H(U_n)), (f(U_n), H, U_1)) \\
&= \sum_{y \in f(\{0,1\}^n)} \Pr[f(U_n) = y] \cdot \mathrm{SD}\big((f(U_n), H, H(U_n) \mid f(U_n) = y) \\
&\qquad\qquad\qquad\qquad\qquad\qquad , (f(U_n), H, U_1 \mid f(U_n) = y)\big) \\
&= \sum_{y \in f(\{0,1\}^n)} \Pr[f(U_n) = y] \cdot \mathrm{SD}\left((y, H, H(X_y)), (y, H, U_1)\right) \\
&\leq \max_{y \in f(\{0,1\}^n)} \mathrm{SD}((y, H, H(X_y)), (y, H, U_1)) \\
&\leq \max_{y \in f(\{0,1\}^n)} \mathrm{SD}((H, H(X_y)), (H, U_1))
\end{aligned}
$$

Proving Claim 8 cont.

Since $\mathrm{H}_\infty(X_y) = \log(d(n))$ for any $y \in \{f(x) \colon x \in \{0,1\}^n)\}$,

Proving Claim 8 cont.

Since $\mathrm{H}_\infty(X_y) = \log(d(n))$ for any $y \in \{f(x) \colon x \in \{0,1\}^n)\}$,
The leftover hash lemma yields that

$$\begin{aligned} \mathrm{SD}((y, H, H(X_y)), (y, H, U_1)) &\leq 2^{(1-\mathrm{H}_\infty(X_y)-2))/2} \\ &= 2^{-(\log d(n)+1)/2} = \mathrm{neg}(n). \quad \square \end{aligned}$$

Further remarks

Remark 9

- We can output $\Theta(\log d(n))$ bits,
- g and b are not defined over all input length.